REMARKS

We have amended the claims to address the Examiner's §112 concerns. More specifically we have made clear what entities are doing what in claims 1 and 11.

We have also canceled claims 2, 6-9, 12, 15, 16, 19-51. And have added claims 52-90, of which claims 54 and 70 are independent method claims. Claim 54 is directed to what takes place on the server side and claim 70 is directed to what takes place on the client side.

The Examiner rejected claims 1, 2, 5-7, 9, 11, 25-29, 33, 34, 36, 42, 44-47, 49, and 50 under 35 U.S.C.§102(e) as anticipated by Holloway (U.S. 6,424,718). Contrary to what the Examiner appears to believe Holloway does not, however, teach the following limitations of claim 1:

> (c) receiving authentication information; and
> (d) providing decryption information for said personal security device responsive to said authentication information.

In essence, Holloway sends an applet to the user in response to the user accessing a particular web page. The applet contains a private key that is encrypted. In order to access the private key, the user must enter a pass-phrase, which only the correct recipient is assumed to know. That is, only the recipient that knows the pass-phrase can access the private key. Any unintended recipients that receive the applet will not know the pass-phrase that is required to access the private key. Holloway states this in the following passages:

> In operation, when a user claiming to be authorised accesses WWW page 135 on web server 136 via browser 105 on client 110, server system 130 compiles applet Ap. Applet Ap includes the claimed users encrypted private key E.sub.PPu (SKu) stored on key server 138, and all of the associated cryptographic algorithms. Server 130 send applet Ap to browser 105 via WWW 100. At browser 105, private key SKu may be used by the applet only if the claimed user knows, and is therefore able to enter into client 110, the owning users pass phrase PPu. Knowledge of pass-phrase PPu establishes the identity of the owning user by enabling use of private key SKu to "sign" messages. (Col. 7, lines 48-59)

> When wishing to request a transaction such as debit instruction, user 150 initially enters his or her identity to client 100. The identity is sent by applet Ap to server systems 130 in enciphered form as hereinbefore described with respect to registration. Server 130 returns the enciphered private key record as hereinbefore described again with respect to registration stage (although now no consent in [sic] required). The private key record is now held by applet Ap in client 110 but still enciphered under pass PPu phrase of user 150. Applet Ap requests user 150 to enter pass-phrase PPu to allow the applet Ap to decipher the private key record in preparation for use. (Col. 9, lines 14-27).

In Holloway, the server does not provide decryption information for the encrypted private key either in response to receiving authentication information or otherwise.

The Examiner characterizes PPu (i.e., the pass-phrase) as authentication information. But PPu is simply used to decipher the enciphered private key record that is within the applet, which was sent to the client something. The server system does not receive PPu as authentication information. Indeed, the server system does not receive PPu as any part of the exchange that takes place between the client and the server system.

With regard to claim 11, Holloway does not teach or suggest "receiving from a key server decryption information for said personal security device," as is required by that claim. As noted above, in connection with claim 1, the pass-phrase, which is the information needed to decipher the enciphered private key is already in the possession of the client. So, for at least that reason claim 11 is patentable over Holloway.

The Examiner also rejected claims 11-13, 15, 16, 19, and 21-24 under 35 U.S.C. §102(e) as being anticipated by Kaufman et al. (U.S. 5,491,752). With regard to claim 11, however, we note Kaufman et al. do not disclose a client receiving both a personal security device and decryption information for decrypting device, as required by this claim. Indeed, Kaufman et al. is directed to a system that is designed to avoid having to send both encrypted information (e.g. a message encrypted by using the session key) and the key used to encrypt that message (i.e., the session key) to the other party. So, Kaufman et al. have designed a system in which both parties are able to separately compute a session key (i.e., the key used for encrypting) based on minimal communication by using knowledge that they both share. (See, Col. 11, lines 44-55).

Since claims 54 and 70 are similar to claims 1 and 11, they are both patentable at least for the same reasons. More specifically, in the case of claim 54 (corresponding generally to claim 1), Holloway does not disclose "as a consequence of authenticating the client, sending a key from a key server to the client, said key for decrypting the identified encrypted container to access the secure information." In the Holloway system, it is assumed that the client already has the key for decrypting the enciphered private key.

In addition, claim 54 also recites a further limitation that is neither taught nor suggested by Holloway, namely:

> at an authentication server, receiving from the client a key query including authentication information;

In the Holloway system, the client simply goes to the appropriate web site and signs in. In response, the server system sends an applet containing an enciphered private key. The client does not send a key query including authentication information to the server system. Moreover, the server system that sends the applet to the client does not authenticate the client, as is also required by claim 54. As the Examiner seems to have appreciated, any authentication that occurs in the Holloway system occurs at the client side of the connection when the user enters a pass-phrase to decipher the enciphered private key. Only the intended user will know the pass-phrase and be able to gain access to the private key.

In the case of claim 70 is patentable for at least the same reasons that claim 11 is patentable. More specifically, Holloway does not disclose:

> in response to sending the authentication information to the authentication server, receiving from a key server a key for decrypting the encrypted container

as required by the claim. In addition, the client in Holloway's system does not send "a key request including authentication information to an authentication server" as is also required by claim 70. Holloway assumes that the client already has the key that is required to decipher the enciphered private key which it sends to the client. And, as noted above, the server system does no authentication of the client, so the client does not need to send authentication information to the server system.

With regard to the teachings of Kaufman et al. we further note that the reference does not teach:

> sending a key request including authentication information to an authentication server;
>
> in response to sending the authentication information to the authentication server, receiving from a key server a key for decrypting the encrypted container

as required by claim 70.

For the reasons stated above, we believe that the claims are allowable and therefore ask the Examiner to allow them to issue.

Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,

Date: April 6, 2004

Eric L. Prahl
Reg. No. 32,590

Hale and Dorr LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6000
Facsimile: (617) 526-5000